Amendments to the Claims

1. (currently amended) A cryptography engine for performing cryptographic operations on an initial input data bit sequence, the initial input data bit sequence having a right portion and a left portion ~~a data block~~, ~~a first portion of the data block occupying a first position and a second portion of the data block occupying a second position,~~ the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

[[a]] two-level multiplexer circuitry including ~~a multiplexer on a first level coupled to a multiplexer on a second level~~

a first level having a first 2-1 multiplexer and a second 2-1 multiplexer, wherein the first 2-1 multiplexer receives the left portion of the initial input data bit sequence at a first input and a right portion of the input bit sequence for a previous cryptographic round at a second input and wherein the second 2-1 multiplexer receives the right portion of the initial input data bit sequence at a first input and the right portion of the input bit sequence for the previous cryptographic round at a second input, and

a second level having a third 2-1 multiplexer and a fourth 2-1 multiplexer, wherein the third 2-1 multiplexer receives the output of the first 2-1 multiplexer at a first input and a right portion of an output bit sequence for a previous cryptographic round at a second input and wherein the fourth 2-1 multiplexer receives the output of the second 2-1 multiplexer at a first input and a right portion of the output bit sequence for the previous cryptographic round at a second input;

expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to the ~~first~~ right portion of the initial input data bit sequence ~~data block occupying the first position~~;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the right portion of the output bit sequence for the previous cryptographic round; ~~first portion of the data block~~, ~~wherein the multiplexer on the first level selects initial input data responsive to a first signal, and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing~~

a substitution box (SBox) configured to transform a third bit sequence to a fourth bit sequence,

wherein the right portion of the output bit sequence for the current cryptographic round is the exclusive OR of the output of the third 2-1 multiplexer and the fourth bit sequence and the left portion of the output bit sequence for the current cryptographic round is the output of the fourth 2-1 multiplexer, and

wherein the two-level multiplexer is configured to swap the left portion of the output bit sequence of a previous cryptographic round with the right portion of the output bit sequence of the previous cryptographic round.

2. (canceled)

3. (original) The cryptography engine of claim 1, wherein the cryptography engine is a DES engine.

4. (canceled)

5. (original) The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. (original) The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7 - 8. (canceled)

9. (original) The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

10. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a plurality of stages.

11. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

12. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a shift stage.

13. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

14. (original) The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

15. (currently amended) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on an initial input data bit sequence, the initial input data bit sequence having a right portion and a left portion ~~a data block,~~ ~~a first portion of the data block occupying a first position and a second portion of the data block occupying a second position~~, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

[[a]] two-level multiplexer circuitry including ~~a multiplexer on a first level coupled to a multiplexer on a second level~~

a first level having a first 2-1 multiplexer and a second 2-1 multiplexer, wherein the first 2-1 multiplexer receives the left portion of the initial input data bit sequence at a first input and a right portion of the input bit sequence for a previous cryptographic round at a second input and wherein the second 2-1 multiplexer receives the right portion of the initial input data bit sequence at a first input and the right portion of the input bit sequence for the previous cryptographic round at a second input, and

a second level having a third 2-1 multiplexer and a fourth 2-1 multiplexer, wherein the third 2-1 multiplexer receives the output of the first 2-1 multiplexer at a first input and a right portion of an output bit sequence for a previous cryptographic round at a second input and wherein the fourth 2-1 multiplexer receives the output of the second 2-1 multiplexer at a first input and a right portion of the output bit sequence for the previous cryptographic round at a second input;

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to the ~~first~~ right portion of the initial input data bit sequence ~~data block occupying the first position~~;

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the right portion of the output bit sequence for the previous cryptographic round; ~~first portion of the data block, wherein the multiplexer on the first level selects initial input data responsive to a first signal, and the multiplexer on the second level receives and associates, in response to a second signal, feedback data from a previous round of cryptographic processing, with the second position, for a next round of cryptographic processing~~

a substitution box (SBox) configured to transform a third bit sequence to a fourth bit sequence, wherein the right portion of the output bit sequence for the current cryptographic round is the exclusive OR of the output of the third 2-1 multiplexer and the fourth bit sequence and the left portion of the output bit sequence for the current cryptographic round is the output of the fourth 2-1 multiplexer, and

wherein the two-level multiplexer is configured to swap the left portion of the output bit sequence of a previous cryptographic round with the right portion of the output bit sequence of the previous cryptographic round.

16. (canceled)

17. (original) The integrated circuit layout of claim 15, wherein the cryptography engine is a DES engine.

18. (canceled)

19. (original) The integrated circuit layout of claim 15, wherein the first bit sequence is less than 32 bits.

20. (currently amended) The integrated ~~integrate~~ circuit layout of claim 15, wherein the first bit sequence is four bits.

21-22. (canceled)

23. (original) The integrated circuit layout of claim 15, wherein the key scheduler performs pipelined key scheduling logic.

24. (original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a plurality of stages.

25. (original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a determination stage.

26. (original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a shift stage.

27. (original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a propagation stage.

28. (original) The integrated circuit layout of claim 15, wherein the key scheduler comprises a consumption stage.

29-40. (canceled)

41. (new) The cryptography engine of claim 1, wherein the cryptographic engine is configured to perform triple-DES.

42. (new) The cryptography engine of claim 41, wherein the two-level multiplexer is configured to select the right portion of a final round of a previous 16-round DES operation as the right portion of the input bit sequence for a first round of a subsequent 16-round DES operation and to select the left potion of the final round of the previous 16-round DES operation as the left portion of the input bit sequence for the first round of the subsequent 16-round DES operation.

43. The cryptography engine of claim 1, wherein the two-level multiplexer is configured to select the right portion of the initial input data bit sequence as the right portion of the input bit sequence for an initial round of a multiple round DES operation and the left portion of the initial input data bit sequence as the left portion of the input bit sequence for the initial round of the multiple round DES operation.

44. (new) The cryptography engine of claim 1, wherein the right portion of the initial input bit sequence is an inverse permutation of a first portion of an input data block and the left portion of the initial input bit sequence is an inverse permutation of a second portion of the input data block.

45. (new) The cryptography engine of claim 1, further including:

a 3-1 multiplexer, wherein the 3-1 multiplexer is configured to receive an initialization vector at a first input, a static vector at a second input, and an output of a cryptographic operation having a plurality of cryptographic rounds; and exclusive OR circuitry coupled to the 3-1 multiplexer, wherein the exclusive OR circuitry is configured to generate the initial input bit sequence as the exclusive OR of an input data block and an output of the 3-1 multiplexer.

46. (new) The integrated circuit layout of claim 15, wherein the cryptographic engine is configured to perform triple-DES.

47. (new) The integrated circuit layout of claim 46, wherein the two-level multiplexer is configured to select the right portion of a final round of a previous 16-round DES operation as the right portion of the input bit sequence for a first round of a subsequent 16-round DES operation and to select the left potion of the final round of the previous 16-round DES operation as the left portion of the input bit sequence for the first round of the subsequent 16-round DES operation.

48. The integrated circuit layout of claim 15, wherein the two-level multiplexer is configured to select the right portion of the initial input data bit sequence as the right portion of the input bit sequence for an initial round of a multiple round DES operation and the left portion of the initial input data bit sequence as the left portion of the input bit sequence for the initial round of the multiple round DES operation.

49. (new) The integrated circuit layout of claim 1, wherein the right portion of the initial input bit sequence is an inverse permutation of a first portion of an input data

block and the left portion of the initial input bit sequence is an inverse permutation of a second portion of the input data block.

50. (new) The integrated circuit layout of claim 15, further including:

a 3-1 multiplexer, wherein the 3-1 multiplexer is configured to receive an initialization vector at a first input, a static vector at a second input, and an output of a cryptographic operation having a plurality of cryptographic rounds; and

exclusive OR circuitry coupled to the 3-1 multiplexer, wherein the exclusive OR circuitry is configured to generate the initial input bit sequence as the exclusive OR of an input data block and an output of the 3-1 multiplexer.